Cisco IOS Zone-basierte Firewall: Büro mit Cisco Unity Express/SRST/PSTN Gateway mit Verbindung zum zentralen Cisco CallManager

Inhalt

Einführung

Cisco Integrated Service Router (ISRs) bieten eine skalierbare Plattform für die Erfüllung der Anforderungen von Daten- und Sprachnetzwerken für eine Vielzahl von Anwendungen. Obwohl die Bedrohungslandschaft von privaten und mit dem Internet verbundenen Netzwerken sehr dynamisch ist, bietet die Cisco IOS® Firewall Funktionen für Stateful Inspection und Application Inspection and Control (AIC), mit denen ein sicherer Netzwerkstatus definiert und durchgesetzt werden kann. Gleichzeitig werden Geschäftsfunktionen und Kontinuität sichergestellt.

In diesem Dokument werden Design- und Konfigurationserwägungen für Firewall-Sicherheitsaspekte bestimmter Cisco ISR-basierter Daten- und Sprachanwendungen beschrieben. Konfiguration für Sprachservices und Firewall wird für jedes Anwendungsszenario bereitgestellt. In jedem Szenario werden die VoIP- und Sicherheitskonfigurationen separat und dann über die gesamte Router-Konfiguration beschrieben. Ihr Netzwerk kann eine andere Konfiguration für Services wie QoS und VPN erfordern, um die Sprachqualität und Vertraulichkeit aufrechtzuerhalten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Cisco IOS Firewall - Hintergrund

Die Cisco IOS Firewall wird in der Regel in Anwendungsszenarien bereitgestellt, die sich von den Bereitstellungsmodellen der Appliance-Firewalls unterscheiden. Typische Bereitstellungen sind Telearbeiter-Anwendungen, Anwendungen für kleine oder Zweigstellen sowie Anwendungen für den Einzelhandel, bei denen eine niedrige Geräteanzahl, die Integration mehrerer Services sowie eine geringere Leistung und Sicherheit gewünscht sind.

Während die Anwendung von Firewall-Inspektionen zusammen mit anderen integrierten Services in den ISR-Produkten aus Kosten- und betrieblicher Sicht attraktiv erscheinen kann, müssen spezifische Überlegungen angestellt werden, um festzustellen, ob eine Router-basierte Firewall geeignet ist. Die Anwendung jeder zusätzlichen Funktion verursacht Speicher- und Verarbeitungskosten und trägt wahrscheinlich zu niedrigeren Weiterleitungsdurchsätzen, einer höheren Paketlatenz und einem Funktionsverlust in Zeiten mit Spitzenauslastung bei, wenn eine nicht ausgelastete integrierte Router-basierte Lösung bereitgestellt wird. Beachten Sie bei der Entscheidung zwischen einem Router und einer Appliance die folgenden Richtlinien:

- Router mit mehreren integrierten Funktionen eignen sich am besten für Zweigstellen- oder Telearbeiter-Standorte, bei denen weniger Geräte eine bessere Lösung bieten.
- Hochleistungsanwendungen mit hoher Bandbreite werden in der Regel besser mit Appliances adressiert. Die Cisco ASA und der Cisco Unified Call Manager-Server sollten für die Anwendung von NAT- und Sicherheitsrichtlinien und die Anrufverarbeitung verwendet werden, während die Router die Anforderungen an QoS-Richtlinienanwendung, WAN-Terminierung und Site-to-Site-VPN-Verbindungen erfüllen.

Vor der Einführung der Cisco IOS Software, Version 12.4(20)T, war die klassische Firewall und die zonenbasierte Policy Firewall (ZFW) nicht in der Lage, die für VoIP-Datenverkehr und routerbasierte Sprachdienste erforderlichen Funktionen vollständig zu unterstützen. Sie erforderten große Öffnungen in ansonsten sicheren Firewall-Richtlinien, um Sprachdatenverkehr aufzunehmen, und sie boten nur begrenzte Unterstützung für neue VoIP-Signalisierungs- und Medienprotokolle.

Konfiguration

Bereitstellung der zonenbasierten Cisco IOS Policy Firewall

Cisco IOS Zone-Based Policy Firewall kann, ähnlich wie andere Firewalls, nur dann eine sichere Firewall bereitstellen, wenn die Sicherheitsanforderungen des Netzwerkvertrauens durch Sicherheitsrichtlinien identifiziert und beschrieben werden. Es gibt zwei grundlegende Ansätze für eine Sicherheitsrichtlinie: im Gegensatz zur *verdächtigen* Perspektive.

Die *vertrauensvolle* Perspektive geht davon aus, dass der gesamte Datenverkehr vertrauenswürdig ist, mit Ausnahme des Datenverkehrs, der als schädlich oder unerwünscht identifiziert werden kann. Es wird eine spezifische Richtlinie implementiert, die nur den unerwünschten Datenverkehr blockiert. Dies wird in der Regel mithilfe spezifischer Zugriffskontrolleinträge oder signatur- oder verhaltensbasierter Tools erreicht. Dieser Ansatz beeinträchtigt in der Regel weniger bestehende Anwendungen, erfordert jedoch ein umfassendes Verständnis der Bedrohungs- und Schwachstellenlandschaft und erfordert eine ständige Wachsamkeit, um neue Bedrohungen und Exploits so anzugehen, wie sie auftreten. Darüber hinaus muss die Benutzer-Community eine große Rolle bei der Gewährleistung angemessener Sicherheit spielen. Eine Umgebung, die weit reichende Freiheit und wenig Kontrolle für die Bewohner ermöglicht, bietet erhebliche Möglichkeiten für Probleme, die durch unvorsichtige oder böswillige Personen verursacht werden. Ein weiteres Problem dieses Ansatzes besteht darin, dass er wesentlich stärker auf effektive Verwaltungstools und Anwendungskontrollen angewiesen ist, die genügend Flexibilität und Leistung bieten, um verdächtige Daten im gesamten Netzwerkverkehr überwachen und kontrollieren zu können. Technologie ist zwar derzeit verfügbar, um diesem Problem zu begegnen, der betriebliche Aufwand übersteigt jedoch häufig die Grenzen der meisten Unternehmen.

Die *verdächtige* Perspektive geht davon aus, dass der gesamte Netzwerkverkehr unerwünscht ist, mit Ausnahme des speziell identifizierten *guten* Datenverkehrs. Dabei handelt es sich um eine Richtlinie, die den gesamten Anwendungsdatenverkehr außer dem explizit zulässigen Datenverkehr blockiert. Zusätzlich kann die Anwendungsinspektion und -kontrolle implementiert werden, um schädlichen Datenverkehr zu identifizieren und zu verweigern, der speziell für die Nutzung *guter* Anwendungen entwickelt wurde, sowie unerwünschten Datenverkehr, der als *guter* Datenverkehr getarnt ist. Auch hier verursachen Anwendungskontrollen betriebliche und leistungsbedingte Belastungen des Netzwerks, obwohl der größte Teil des unerwünschten Datenverkehrs durch Stateless-Filter wie Zugriffskontrolllisten (ACLs) oder ZFW-Richtlinien (Zone-Based Policy Firewall) gesteuert werden sollte. Auf diese Weise sollte der Datenverkehr durch AIC, ein Intrusion Prevention System (IPS) oder andere signaturbasierte Kontrollen wie Flexible Packet Matching (FPM) oder netzwerkbasierte Anwendungserkennung (NNIPS) reduziert werden. LEISTE). Wenn also nur die gewünschten Anwendungsports und der dynamische medienspezifische Datenverkehr, der durch bekannte Steuerungsverbindungen oder Sitzungen erzeugt wird, ausdrücklich zugelassen werden, sollte der einzige unerwünschte Datenverkehr, der im Netzwerk vorhanden sein sollte, in eine bestimmte, leichter erkennbare Teilmenge fallen, wodurch der technische und betriebliche Aufwand für die Aufrechterhaltung der Kontrolle über unerwünschten Datenverkehr verringert wird.

In diesem Dokument werden VoIP-Sicherheitskonfigurationen basierend auf *verdächtigen* Aspekten beschrieben. Somit ist nur der in den Sprachnetzsegmenten zulässige Datenverkehr zulässig. Datenrichtlinien sind tendenziell permissiver, wie in den Notizen in der Konfiguration der einzelnen Anwendungsszenarien beschrieben.

Bei allen Bereitstellungen von Sicherheitsrichtlinien muss ein Kreislauf-Feedback-Zyklus eingehalten werden. Sicherheitsbereitstellungen wirken sich in der Regel auf die Funktionen und Funktionen vorhandener Anwendungen aus und müssen angepasst werden, um diese Auswirkungen zu minimieren oder zu beheben.

Weitere Informationen und zusätzliche Hintergrundinformationen zur Konfiguration der zonenbasierten Policy Firewall-Firewall finden Sie im Design- und Anwendungshandbuch für zonenbasierte Richtlinien.

Überlegungen zur ZFW in VoIP-Umgebungen

Der zuvor erwähnte Design- und Anwendungsleitfaden bietet eine kurze Erläuterung der Sicherheit des Routers unter Verwendung von Sicherheitsrichtlinien für die und aus der Selbstzone des Routers sowie alternativer Funktionen, die über verschiedene NFP-Funktionen (Network Foundation Protection) bereitgestellt werden. Router-basierte VoIP-Funktionen werden in der Selbstzone des Routers gehostet. Sicherheitsrichtlinien, die den Router schützen, müssen die Anforderungen für Sprachdatenverkehr berücksichtigen, um die Sprachsignalisierung und die Medien zu integrieren, die von Cisco Unified CallManager Express, Survivable Remote Site Telefony und Voice Gateway-Ressourcen generiert wurden und für diese bestimmt sind. Vor der Cisco IOS Software-Version 12.4(20)T waren die klassische Firewall und die zonenbasierte Firewall nicht in der Lage, die Anforderungen des VoIP-Datenverkehrs vollständig zu erfüllen, sodass die Firewall-Richtlinien nicht für den vollständigen Schutz der Ressourcen optimiert wurden. Sicherheitsrichtlinien für die Selbstzone zum Schutz routerbasierter VoIP-Ressourcen basieren in hohem Maße auf Funktionen der Cisco IOS Software, Version 12.4(20)T.

Sprachfunktionen der Cisco IOS Firewall

In der Cisco IOS Software, Version 12.4(20)T, wurden verschiedene Verbesserungen eingeführt, um gleichzeitig vorhandene Zone-Firewall- und Sprachfunktionen zu aktivieren. Drei Hauptfunktionen gelten direkt für sichere Sprachanwendungen:

- SIP-Erweiterungen: Gateway und Anwendungsinspektion und -kontrolle auf AnwendungsebeneAktualisierungen der SIP-Versionsunterstützung für SIPv2, wie in RFC 3261 beschriebenUnterstützung für SIP-Signalisierung zur Erkennung einer größeren Vielfalt von AnrufströmenEinführung von SIP Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf AnwendungsebeneErweiterung der Selbstzonenüberprüfung, um sekundäre Signalisierungs- und Medienkanäle erkennen zu können, die aus lokal bestimmtem/vom SIP-Datenverkehr ausgehenden Datenverkehr stammen
- Unterstützung für lokalen Skinny-Datenverkehr und Cisco CallManager ExpressAktualisiert SCCP-Unterstützung auf Version 16 (zuvor unterstützte Version 9)Einführung von SCCP Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf AnwendungsebeneErweiterung der Selbstzonenprüfung, um sekundäre Signalisierungs- und Medienkanäle erkennen zu können, die aus lokal bestimmtem SCCP-Datenverkehr mit Ursprung in zu erkennen sind
- H.323 v3/v4-UnterstützungAktualisierung der H.323-Unterstützung für v3 und v4 (zuvor unterstützt v1 und v2), wie unter beschriebenEinführung von H.323 Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf Anwendungsebene

Die in diesem Dokument beschriebenen Router-Sicherheitskonfigurationen umfassen Funktionen, die von diesen Erweiterungen angeboten werden, und erläutern, wie die von den Richtlinien angewendeten Aktionen beschrieben werden. Hyperlinks zu den einzelnen Funktionsdokumenten finden Sie im Abschnitt Zugehörige Informationen am Ende dieses Dokuments, wenn Sie die vollständigen Details zu den Sprachprüfungsfunktionen überprüfen möchten.

Hinweise

Die Anwendung der Cisco IOS Firewall mit routerbasierten Sprachfunktionen muss die zonenbasierte Policy Firewall anwenden, um die zuvor erwähnten Punkte zu untermauern. Die klassische IOS-Firewall bietet nicht die erforderliche Funktion zur vollständigen Unterstützung der Komplexität und des Verhaltens von Sprachdatenverkehr bei der Signalisierung.

NAT

Cisco IOS Network Address Translation (NAT) wird häufig gleichzeitig mit der Cisco IOS Firewall konfiguriert, insbesondere in Fällen, in denen private Netzwerke mit dem Internet verbunden werden müssen oder in denen unterschiedliche private Netzwerke eine Verbindung herstellen müssen, insbesondere wenn sich überschneidende IP-Adressräume genutzt werden. Die Cisco IOS Software umfasst NAT-Application-Layer-Gateways (ALGs) für SIP, Skinny und H.323. Im Idealfall kann die Netzwerkkonnektivität für IP-Sprache ohne Anwendung von NAT genutzt werden, da NAT die Fehlerbehebung und Sicherheitsrichtlinienanwendungen zusätzlich vereinfacht, insbesondere bei Verwendung von NAT-Überlastung. NAT sollte nur als letzte Lösung zur Behebung von Netzwerkverbindungsproblemen angewendet werden.

CUPC

In diesem Dokument wird keine Konfiguration beschrieben, die die Verwendung von Cisco Unified Presence Client (CUPC) mit der Cisco IOS Firewall unterstützt, da CUPC noch nicht von Zone oder klassischer Firewall unterstützt wird, wie in der Cisco IOS Software, Version 12.4(20)T1. CUPC wird in einer zukünftigen Version der Cisco IOS Software unterstützt.

Büro mit Cisco Unity Express/SRST/PSTN Gateway für die Verbindung mit dem zentralen Cisco CallManager

Dieses Szenario unterscheidet sich von den vorherigen Anwendungen, da die zentrale Anrufsteuerung für die gesamte Anrufsteuerung statt für die verteilte routerbasierte Anrufverarbeitung verwendet wird. Verteilte Voicemail wird angewendet, jedoch über Cisco Unity Express auf dem Router. Der Router bietet Survivable Remote Site Telefony und PSTN Gateway-Funktionen für Notruf- und Ortsgespräche. Es wird empfohlen, eine anwendungsspezifische PSTN-Kapazität bereitzustellen, um den Ausfall des WAN-basierten Umgehungswählsowie des Ortsgesprächs, wie im Wählplan beschrieben, zu bewältigen. Darüber hinaus müssen laut lokalen Gesetzen normalerweise lokale PSTN-Verbindungen bereitgestellt werden, um Notrufe (911) zu ermöglichen.

In diesem Szenario kann Cisco CallManager Express auch als Anrufverarbeitungsagent für SRST angewendet werden, falls bei WAN-/CCM-Ausfällen eine größere Anrufverarbeitungsfunktion erforderlich ist. Weitere Informationen finden Sie unter Integration von Cisco Unity Connection mit Cisco Unified CME-as-SRST.

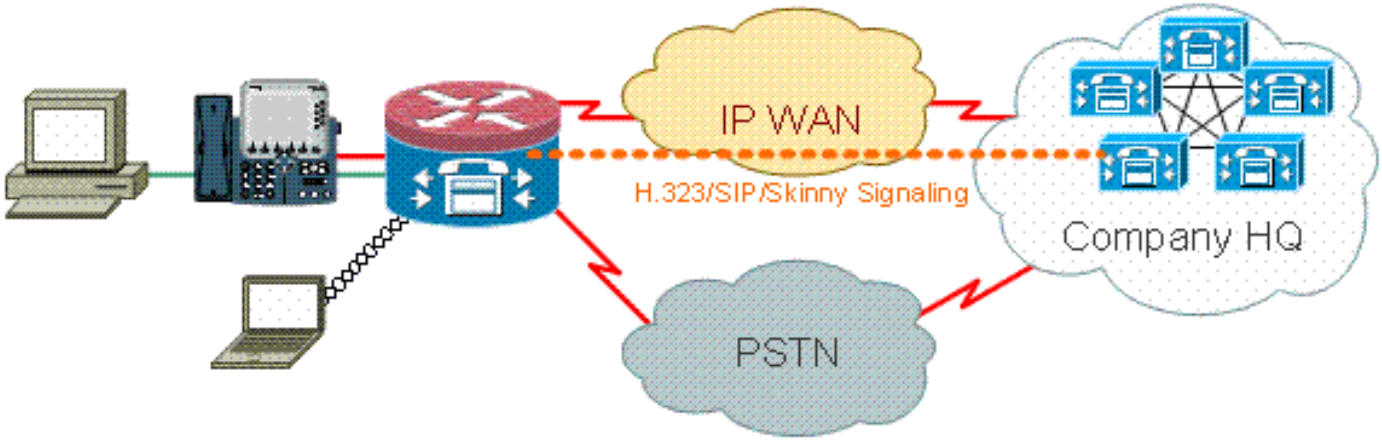
Szenario-Hintergrund

Das Anwendungsszenario umfasst kabelgebundene Telefone (Sprach-VLAN), verkabelte PCs (Daten-VLAN) und Wireless-Geräte (einschließlich VoIP-Geräte wie IP Communicator).

1. Signalisierungsprüfung zwischen lokalen Telefonen und Remote-CUCM-Cluster (SCCP und

SIP)

2. Untersuchen Sie die H.323-Signalisierung zwischen dem Router und dem Remote-CUCM-Cluster.
3. Untersuchen Sie die Signalisierung zwischen den lokalen Telefonen und dem Router, wenn die Verbindung zum Remote-Standort unterbrochen und die SRST aktiv ist.
4. Sprachmedien-Pinholes für die Kommunikation zwischen:Lokale kabelgebundene und Wireless-SegmenteLokale und Remote-TelefoneRemote-Warteschleifenmusik-Server und lokale TelefoneRemote-Unity-Server und lokale Telefone für Voicemail
5. Application Inspection and Control (AIC) auf:Übertragungsratenlimit für Einladungendie Protokollkonformität für den gesamten SIP-Datenverkehr sicherstellen.



Vorteile/Nachteile

Dieses Szenario bietet den Vorteil, dass der Großteil der Anrufverarbeitung in einem zentralen Cisco CallManager-Cluster erfolgt, was den Verwaltungsaufwand verringert. Der Router sollte im Vergleich zu den anderen in diesem Dokument beschriebenen Fällen in der Regel weniger lokale Sprachressourcen-Überprüfungslast bewältigen müssen, da der Großteil der Anrufverarbeitungslast nicht auf den Router entfällt, außer bei der Verarbeitung des Datenverkehrs vom/zum Cisco Unity Express, und in Fällen, in denen ein WAN- oder CUCM-Ausfall vorliegt und lokale Cisco CallManager Express/SRST-Verbindungen zur Anrufverarbeitung eingesetzt werden.

Der größte Nachteil dieses Falls ist, dass sich Cisco Unity Express bei einer typischen Anrufverarbeitungsaktivität auf dem lokalen Router befindet. Auch wenn dies aus konzeptioneller Sicht gut ist: Cisco Unity Express befindet sich am nächsten an den Endbenutzern, an denen Voicemail gespeichert wird, verursacht jedoch einen zusätzlichen Verwaltungsaufwand, da eine große Anzahl von Cisco Unity Express verwaltet werden kann. Mit einem zentralen Cisco Unity Express, der die gegenteiligen Nachteile mit sich bringt, ist ein zentrales Cisco Unity Express jedoch weiter von Remote-Benutzern entfernt und bei Ausfällen möglicherweise nicht zugänglich. Die funktionalen Vorteile der verteilten Voicemail, die durch die Bereitstellung von Cisco Unity Express an Remote-Standorten bereitgestellt werden, bieten somit eine hervorragende Wahl.

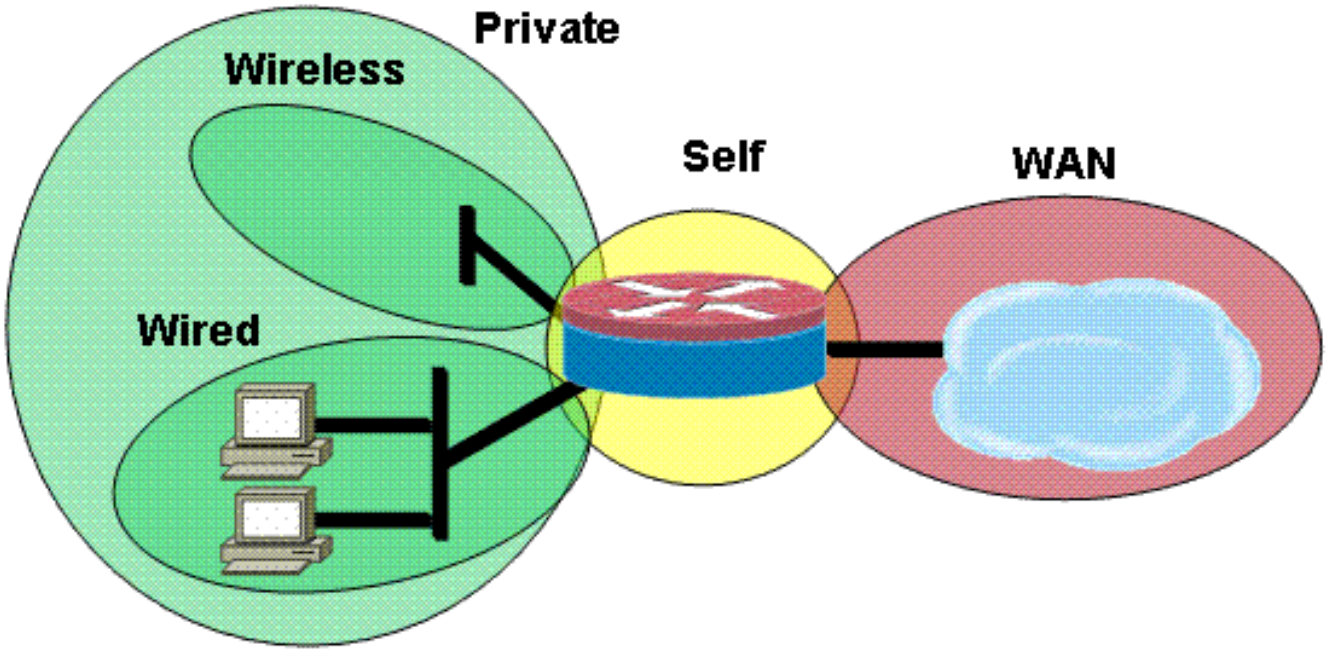
Konfigurationen für Datenrichtlinien, zonenbasierte Firewall, Sprachsicherheit, Cisco CallManager Express

Die Router-Konfiguration basiert auf einem 3845 mit einem NME-X-23ES und einer PRI HWIC:

Konfiguration von Sprachdiensten für SRST- und Cisco Unity Express-Konnektivität:

```
!
telephony-service
 load 7960-7940 P00308000400
 max-ephones 24
 max-dn 24
 ip source-address 192.168.112.1 port 2000
 system message CME2
 max-conferences 12 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Jun 10 2008 15:47:13
!
```

Dies ist ein Beispiel für die zonenbasierte Firewall-Konfiguration, die aus Sicherheitszonen für kabelgebundene und Wireless-LAN-Segmente, einem privaten LAN besteht, das aus kabelgebundenen und Wireless-Segmenten besteht, einem WAN-Segment, in dem vertrauenswürdige WAN-Verbindungen erreicht werden, und der Selbstzone, in der sich die Sprachressourcen des Routers befinden:



Sicherheitskonfiguration:

```
class-map type inspect match-all acl-cmap
 match access-group 171
class-map type inspect match-any most-traffic-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
!
!
policy-map type inspect most-traffic-pmap
 class type inspect most-traffic-cmap
  inspect
 class class-default
  drop
policy-map type inspect acl-pass-pmap
 class type inspect acl-cmap
  pass
!
```

```
zone security private
zone security public
zone security wired
zone security wireless
!
zone-pair security priv-pub source private destination public
 service-policy type inspect most-traffic-pmap
zone-pair security priv-vpn source private destination vpn
 service-policy type inspect most-traffic-pmap
zone-pair security acctg-pub source acctg destination public
 service-policy type inspect most-traffic-pmap
zone-pair security eng-pub source eng destination public
 service-policy type inspect most-traffic-pmap
!
!
!
interface GigabitEthernet0/0
 ip virtual-reassembly
 zone-member security eng
```

Entire router configuration:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3825-srst
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring
!
dot11 syslog
ip source-route
!
!
ip cef
ip cef
!
!
ip domain name cisco.com
ip name-server 172.16.1.22
ip vrf acctg
 rd 0:1
!
ip vrf eng
 rd 0:2
!
ip inspect WAAS enable
!
no ipv6 cef
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!
!
```

```
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
class-map type inspect match-all acl-cmap
 match access-group 171
class-map type inspect match-any most-traffic-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
!
!
policy-map type inspect most-traffic-pmap
 class type inspect most-traffic-cmap
  inspect
 class class-default
  drop
policy-map type inspect acl-pass-pmap
 class type inspect acl-cmap
  pass
!
zone security private
zone security public
zone security vpn
zone security eng
zone security acctg
zone-pair security priv-pub source private destination public
 service-policy type inspect most-traffic-pmap
zone-pair security priv-vpn source private destination vpn
 service-policy type inspect most-traffic-pmap
zone-pair security acctg-pub source acctg destination public
 service-policy type inspect most-traffic-pmap
zone-pair security eng-pub source eng destination public
 service-policy type inspect most-traffic-pmap
!
!
!
!
interface Loopback101
 ip vrf forwarding acctg
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface Loopback102
 ip vrf forwarding eng
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface GigabitEthernet0/0
 no ip address
```

```
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.103 255.255.255.0
 shutdown
!
interface GigabitEthernet0/0.109
 encapsulation dot1Q 109
 ip address 172.16.109.11 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 zone-member security public
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1.129
 encapsulation dot1Q 129
 ip address 172.17.109.2 255.255.255.0
 standby 1 ip 172.17.109.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.109
!
interface GigabitEthernet0/1.149
 encapsulation dot1Q 149
 ip address 192.168.109.2 255.255.255.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nat inside
 ip virtual-reassembly
 zone-member security private
!
interface GigabitEthernet0/1.161
 encapsulation dot1Q 161
 ip vrf forwarding acctg
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface GigabitEthernet0/1.162
 encapsulation dot1Q 162
 ip vrf forwarding eng
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface Serial0/3/0
 no ip address
 encapsulation frame-relay
 shutdown
 frame-relay lmi-type cisco
!
interface Serial0/3/0.1 point-to-point
```

```
 ip vrf forwarding acctg
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 321 IETF
!
interface Serial0/3/0.2 point-to-point
 ip vrf forwarding eng
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 322 IETF
!
interface Integrated-Service-Engine2/0
 no ip address
 shutdown
 no keepalive
!
interface GigabitEthernet3/0
 no ip address
 shutdown
!
router eigrp 1
 network 172.16.109.0 0.0.0.255
 network 172.17.109.0 0.0.0.255
 no auto-summary
!
router eigrp 104
 network 10.1.104.0 0.0.0.255
 network 192.168.109.0
 network 192.168.209.0
 no auto-summary
!
router bgp 1109
 bgp log-neighbor-changes
 neighbor 172.17.109.4 remote-as 1109
 !
 address-family ipv4
  neighbor 172.17.109.4 activate
  no auto-summary
  no synchronization
  network 172.17.109.0 mask 255.255.255.0
 exit-address-family
!
ip forward-protocol nd
ip route vrf acctg 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf acctg 10.1.2.0 255.255.255.0 10.255.1.2
ip route vrf eng 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf eng 10.1.2.0 255.255.255.0 10.255.1.2
!
!
ip http server
no ip http secure-server
ip nat pool acctg-nat-pool 172.16.109.21 172.16.109.22 netmask 255.255.255.0
ip nat pool eng-nat-pool 172.16.109.24 172.16.109.24 netmask 255.255.255.0
ip nat inside source list 109 interface GigabitEthernet0/0.109 overload
ip nat inside source list acctg-nat-list pool acctg-nat-pool vrf acctg overload
ip nat inside source list eng-nat-list pool eng-nat-pool vrf eng overload
```

```
ip nat inside source static 172.17.109.12 172.16.109.12 extendable
!
ip access-list extended acctg-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended eng-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
!
logging 172.16.1.20
access-list 1 permit any
access-list 109 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 109 permit ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
access-list 141 permit ip 10.0.0.0 0.255.255.255 any
access-list 171 permit ip host 1.1.1.1 host 2.2.2.2
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
gateway
 timer receive-rtp 1200
!
!
alias exec sh-sess show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
line aux 0
line 130
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
```

```
 no inservice
!
end
```

Bereitstellung, Verwaltung und Überwachung

Die Bereitstellung und Konfiguration sowohl für Router-basierte IP-Telefonie-Ressourcen als auch für zonenbasierte Richtlinien-Firewall ist im Allgemeinen am besten mit Cisco Configuration Professional kompatibel. Cisco Secure Manager unterstützt keine zonenbasierte Firewall oder routerbasierte IP-Telefonie.

Die Cisco IOS Classic Firewall unterstützt die SNMP-Überwachung mit der Cisco Unified Firewall MIB. Zonenbasierte Richtlinien-Firewall wird von der Unified Firewall-MIB jedoch noch nicht unterstützt. Daher muss die Firewall-Überwachung mithilfe von Statistiken über die Befehlszeilenschnittstelle des Routers oder mithilfe von GUI-Tools wie Cisco Configuration Professional erfolgen.

Das Cisco Secure Monitoring and Reporting System (CS-MARS) bietet grundlegende Unterstützung für die zonenbasierte Policy-Firewall. Es protokolliert jedoch Änderungen, die eine verbesserte Protokollnachrichten-Korrelation mit Datenverkehr bewirken, der in der Cisco IOS Software-Version 12.4(15)T4/T5 und in der Cisco IOS-Softwareversion 12.4(20)T implementiert wurde.

Kapazitätsplanung

Ergebnisse des Firewall Call Inspection Performance Test (TBD) aus Indien.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Die Cisco IOS Zone Firewall stellt **Anzeige**- und **Debugbefehle** bereit, um die Aktivitäten der Firewall anzuzeigen, zu überwachen und Fehler zu beheben. In diesem Abschnitt wird die Verwendung der Befehle **show** zur Überwachung grundlegender Firewall-Aktivitäten sowie eine Einführung in die **Debugbefehle** der Zonenfirewall für eine detailliertere Fehlerbehebung beschrieben, oder wenn die Besprechung mit dem technischen Support detaillierte Informationen erfordert.

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Befehle anzeigen

Die Cisco IOS Firewall bietet mehrere **Show**-Befehle, um die Konfiguration und Aktivität von

Sicherheitsrichtlinien anzuzeigen:

Viele dieser Befehle können mithilfe des **Alias-**Befehls durch einen kürzeren Befehl ersetzt werden.

Debugbefehle

Debug-Befehle können nützlich sein, wenn Sie eine atypische oder nicht unterstützte Konfiguration verwenden und zur Lösung von Interoperabilitätsproblemen mit dem Cisco TAC oder den technischen Support-Services anderer Produkte zusammenarbeiten müssen.

Hinweis: Die Anwendung von **Debug-**Befehlen auf bestimmte Funktionen oder Datenverkehr kann dazu führen, dass eine sehr große Anzahl von Konsolenmeldungen ausgegeben wird, wodurch die Router-Konsole nicht mehr reagiert. Wenn Sie das Debuggen aktivieren müssen, können Sie auch einen anderen Zugriff auf die Befehlszeilenschnittstelle bereitstellen, z. B. ein Telnet-Fenster, das den Terminaldialog nicht überwacht. Sie sollten das Debuggen nur für Offline-Geräte (Laborumgebung) oder während eines geplanten Wartungsfensters aktivieren, da das Debuggen erheblich die Routerleistung beeinflussen kann.

Zugehörige Informationen

- Designleitfaden für das Referenznetzwerk der Cisco Unified CallManager Express-Lösung
- Cisco Unified CallManager Express Security - Best Practices
- Integration von Cisco Unity Connection mit Cisco Unified CME-as-SRST
- Befehlsreferenz für Cisco Unified Communications Manager Express
- Konfigurationsbeispiel für Cisco CallManager Express/Cisco Unity Express
- Cisco CallManager Express 3.4 SNMP MIB-Unterstützung
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Unterstützung der Cisco IOS Firewall für lokalen Skinny-Datenverkehr und CME
- Cisco IOS Firewall
- Technischer Support und Dokumentation für Cisco Systeme